FAUNA & FLORA INTERNATIONAL

ခေါင်းစဉ်	သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ (ICT) မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်း		
စတင်အသက်ဝင်သည့် နေ့စွဲ	ဇွန်လ ၂၀၁၈	အမှတ်	၁
နောက်ဆုံး ပြင်ဆင်ခြင်း	-	ဌာန	စီမံရေးရာ
မူဝါဒ ရေးဆွဲသူ	လင်ဒါ ဘိတ်ကာICT မန်နေဂျာ	ခွင့်ပြုချက်အရ	အကြီးတန်းစီမံခန့်ခွဲမှု အဖွဲ့

ရည်ရွယ်ချက်

FFI သည် ICT ပစ္စည်းများနှင့် ဆက်စပ်ရင်းမြစ်များကို အသုံးပြုရာတွင် ထိရောက်သော ကမ္ဘာလုံးဆိုင်ရာ မူဝါဒကို ကျင့်သုံးကြောင်းသေချာစေရန်ဖြစ်သည်။ မူဝါဒတွင် IT ပစ္စည်းများ အသုံးပြုခြင်း၊ ဝယ်ယူခြင်းနှင့် ရုပ်ပိုင်းဆိုင်ရာ လုံခြုံမှု၊ software ထည့်သွင်းခြင်းများ၊ password လုပ်ထုံးလုပ်နည်းများနှင့် အင်တာနက် လုံခြုံမှုတို့နှင့်ပတ်သက်၍ ရှင်းလင်းစွာ ရေးဆွဲထားသည်။

နယ်ပယ် - ဤမူဝါဒသည်

FFI မှ ပစ္စည်းကိရိယာပေးအပ်ထားသူများအားလုံး၊ FFI လုပ်ငန်းကိစ္စများအတွက် တစ်ကိုယ်ရည် ပစ္စည်းများ အသုံးပြုသူ များနှင့် FFI စနစ်များကို ရယူသုံးစွဲနေရသူများအားလုံး အကျုံးဝင်သည်။ အချိန်မရွေး၊ နေရာမရွေး စနစ်များကို ဝင်ရောက်ရန် ပစ္စည်းသုံးစွဲမှုများအားလုံး အကျုံးဝင်သည်။

မူဝါဒဖော်ပြချက်

ICT သည် FFI လုပ်ငန်းများအတွက် ပေါင်းစပ်အစိတ်အပိုင်းတစ်ခုဖြစ်ပြီး၊ FFI သည် ထိရောက်သော ဆက်သွယ်မှု၊ အချက်အလက်စီမံခန့်ခွဲမှုနှင့် မျှဝေခြင်းနှင့် စီမံနှင့် ငွေကြေးဆိုင်ရာလုပ်ငန်းများ အတွက် သင့် လျော်သော၊ ပေါင်းစပ် ထားသော၊ အထောက်အပံ့ဖြစ်သော ICT ရင်းမြစ်များကို ပံ့ပိုးပေးလျက်ရှိသည်။ FFI သည် လုပ်ငန်းဆိုင်ရာ သုံးစွဲရန် ICT ပစ္စည်းများကိုပံ့ပိုးပေးထားပြီး၊ ထိုပစ္စည်းများကို တစ်ကိုယ်ရည်သုံးစွဲမှု သည် တိုက်ဆိုင်မှုကြောင့်သာ ဖြစ်ရမည်။ FFI သည် နောက်ဆုံးပေါ် ICT ရင်းမြစ်များနှင့် နည်းပညာများကို အသုံးပြုရန်ရည်ရွယ်ထားပြီး၊ တစ်ဆက်တည်းတွင် ဆိုက်ဘာအန္တရာယ်များနှင့် ခြိမ်းခြောက်မှုများကို သတိပြုပြီး ကာကွယ်နေသည်။ FFI မှ ပစ္စည်းကိရိယာ ထောက်ပံ့ထားသူများ၊ FFI လုပ်ငန်းများအတွက် တစ်ကိုယ်ရည်သုံးပစ္စည်းများ အသုံးပြုပြီး အလုပ်လုပ်နေရသူများ သို့မဟုတ် FFI ၏ စနစ်များကို ဝင် ရောက်သုံးစွဲနေရသူများသည် FFI၏ ပစ္စည်းကိရိယာများ၊ အချက်အလက်များနှင့် လုံခြုံမှုကို ကာကွယ်ရန် အတွက် ဤမူဝါဒကိုလိုက်နာရန် လိုအပ်သည်။

တာဝန်ယူမှု

အကြီးတန်းစီမံခန့်ခွဲမှုအဖွဲ့ (SMT) သည် ဤမူဝါဒအကောင်အထည်ဖော်ခြင်းနှင့် လိုက်နာဆောင်ရွက်ခြင်း တို့အတွက် တာဝန်ရှိသည်။ ICT မန်နေဂျာသည် ဤမူဝါဒနှင့်ပတ်သက်ပြီး ဆက်သွယ်ဆက်ဆံခြင်း၊ ဆန်းစစ်ခြင်းနှင့် ပြုပြင်ခြင်း တို့အတွက်တာဝန်ရှိသည်။ အကြီးတန်းစီမံခန့်ခွဲမှုအဖွဲ့(SMT)နှင့်သက်ဆိုင်ရာ မန်နေဂျာများသည် စံနမူနာအဖြစ် လိုက်နာဆောင်ရွက်ပြရန် တာဝန်ရှိသည်။ ဝန်ထမ်းတစ်ဦးချင်းစီလည်း လိုက်နာရန် တာဝန်ရှိသည်။

မူဝါဒကို ချိုးဖောက်ခြင်း

ဤမူဝါဒကို ချိုးဖောက်လျှင် ပြင်းထန်စွာအရေးယူမည်ဖြစ်ပြီး၊ FFI ၏ စည်းကမ်းပိုင်းဆိုင်ရာ လုပ်ထုံးလုပ်နည်းများ အတိုင်း ဆောင်ရွက်သွားမည်။

Hardware/ Software

Hardware

FFI ၏ စံသတ်မှတ်ထားသော operating environment သည် Microsoft Windows ဖြစ်သည်။ Windows operating system ကိုသာ ထောက်ပံ့ထားသည်။ အခြား စနစ်များသည် FFI၏ IT အခြေခံအဆောက်အဦနှင့် မကိုက်ညီနိုင်ပါ။

MAC များ အသုံးပြုခြင်းနှင့် ဝယ်ယူခြင်းကို လုပ်ငန်းသဘောအရ ချွင်းချက်သုံးစွဲခြင်းမှတစ်ပါး ခွင့်မပြုထားပါ။ အကယ်၍ လုပ်ငန်းအတွက်လိုအပ်၍သုံးစွဲရပါက ICT မန်နေဂျာ၏ ခွင့်ပြုချက်ကိုယူရမည်ဖြစ်သည်။ သို့သော် MAC များအတွက် ICT အထောက်အပံ့ကို မပေးနိုင်ပါ။

Software

စစ်မှန်သော၊ လိုင်စင် Windows installed လုပ်ထားသော Laptop များ၊ ကွန်ပျူတာများကိုသာ ဝယ်ယူရမည်။ စနစ်များ ကောင်းစွာအလုပ်လုပ်စေရန် Windows နှင့် Office ကို နောက်ဆုံးပေါ် ဖြစ်နေစေရန် Windows update အားပုံမှန် လုပ် ထားရန် လိုအပ်သည်။

Laptop များ၊ ကွန်ပျူတာများအားလုံးတွင် Webroot anti-virus software ကို install လုပ်ပြီး ပုံမှန် update လုပ်ထား ရမည်။ Webroot ကို မည်သို့ install လုပ်ရမည်ကို MyFFI (Webroot) မှာကြည့်နိုင်ပြီး၊ လမ်းညွှန်မှု အတွက် ICT support ကို ဆက်သွယ်ရယူနိုင်သည်။

FFI ပစ္စည်းကိရိယာများတွင် သွင်းထားသော software များသည် တရားဝင် လုပ်ငန်းများလုပ်ရန် အတွက်သာဖြစ်သည်။ software အားလုံးသည် စစ်မှန်သော၊ လိုင်စင်အပြည့်ပါသော၊ တရားဝင် ရောင်းချသည့်ရင်းမြစ်များထံမှ ဝယ်ယူထားရမည်ဖြစ်ပြီး ပုံမှန် update လုပ်ရမည်။ တရားဝင်ရောင်းချသည့် ရင်းမြစ်ကို သံသယရှိပါက ICT မန်နေဂျာကို ဆက် သွယ်လိုက်ပါ။

အစစ်မှန်မဟုတ်သော software ကို တင်းကြပ်စွာ တားမြစ်ထားသည်။

- ၎င်းသည် တရားမဝင်ဖြစ်ပြီး၊ သုံးစွဲလျှင် FFI ပင်လျှင် တရားစွဲခံရနိုင်သည်

- ၄င်းတွင်Malware ပုံစံမျိုးစုံပါနိုင်ပြီး၊ laptop များ၊ ကွန်ပျူတာများကို ကူးစက်ခံရနိုင်ကာ အခြား ပစ္စည်း ကိရိယာ များနှင့် FFI ကွန်ယက်ကိုပါ ကူးစက်ခံရနိုင်သည်
- Update များကို install လုပ်၍မရနိုင်ဘဲ laptop များ၊ ကွန်ပျူတာများကို အန္တရာယ်ရှိစေနိုင်သည်
- နေ့စဉ်လုပ်ငန်းများ ပြီးမြောက်စေရန် FFI ၏စနစ်များကို ဝင်ရောက်နိုင်ခြင်းမရှိတော့ခြင်းများ ဖြစ်နိုင်သည်။

Software အစစ်အမှန်များကို ရရှိနိုင်ရန် ICT မန်နေဂျာကိုဆက်သွယ်ပါ။ FFI ရုံးချုပ်အနေဖြင့် ပရဟိတ အဖွဲ့အစည်း နှုန်းထားဖြင့် ဝယ်ယူရရှိနိုင်သည်။

Software များကို ခွင့်ပြုချက်မရဘဲ ကူးယူခြင်း၊ ဖြန့်ချိခြင်းများမပြုလုပ်ရပါ။ အကယ်၍ software ကူးယူခြင်းနှင့် ပတ်သက်ပြီး သံသယရှိပါက ICT မန်နေဂျာကို ဆက်သွယ်ပါ။

Internet Protocol (အင်တာနက်ကျင့်ဝတ်)

FFI သည် ရုံးလုပ်ငန်းများအဆင်ပြေချောမွေ့စေရန် အင်တာနက်ကိုပံ့ပိုးပေးထားသည်။ အင်တာနက်ကို မသင့်လျော်သော ရည်ရွယ်ချက်များအတွက် အသုံးမပြုရပါ။ ၄င်းတို့တွင်

- ညစ်ညမ်းသောသဘောရှိသည့် အကြောင်းအရာများကို သိလျက်နှင့် လက်ခံခြင်း၊ ပေးပို့ခြင်းနှင့် ကြည့်ရှုခြင်း
- ပုတ်ခတ်တိုက်ခိုက်မှုဟု ယူဆရနိုင်သော အကြောင်းအရာများကို သိလျက်နှင့် လက်ခံခြင်း၊ ပေးပို့ ခြင်းနှင့် ကြည့်ရှုခြင်း
- ရာဇဝတ်မှု သဘောသဘာဝရှိသော အွန်လိုင်း လှုပ်ရှားမှုများ လုပ်ဆောင်ခြင်း
- မည်သည့် အွန်လိုင်း လောင်းကစားမဆိုပြုလုပ်ခြင်း
- FFI မိတ်ဘက်အဖွဲ့အစည်းများ သို့မဟုတ် ပတ်သက်ဆက်နွယ်သူများအား ဂုဏ်သိက္ခာကျဆင်းစေသော အကြောင်းအရာများကို onlineမှ လုပ်ဆောင်ခြင်း
- အင်တာနက်ကို သင်၏အလုပ်အကိုင် ထိခိုက်အန္တရာယ်ရှိလာသည်အထိ အသုံးပြုခြင်း
- မူပိုင်ခွင့်နှင့် ကာကွယ်ထားသော အရာများကို ချိုးဖောက်ပြီး download ဆွဲခြင်းနှင့်၊ သို့မဟုတ် သတင်းအချက် အလက်များ မျှဝေခြင်း
- FFI စနစ်များ၏ ပြည့်စုံကောင်းမွန်မှုကို ထိခိုက်စေသော အရာများကို download ဆွဲခြင်း (ဥပမာ - သတိပေး ချက် ထုတ်ပြန်ထားပါလျက် virus ပါသော email များကို ဖွင့်ခြင်း)
- FFI ၏ စနစ်များကို ထိခိုက်နိုင်မည်ကို သိလျက်နှင့် မျှဝေခြင်း (virus ပါနိုင်သော အရာများကို မျှဝေခြင်း)
- FFI မိတ်ဘက်အဖွဲ့များ သို့မဟုတ် ပတ်သက်ဆက်နွယ်သူများ၏ ပညာရှင်မဆန်သော ဓာတ်ပုံများကိုဖော်ပြ ခြင်းနှင့်၊ သို့မဟုတ်
- လူမှုကွန်ယက်ကို မသင့်လျော်စွာ အသုံးပြုခြင်း (အသေးစိတ်ကို ဝန်ထမ်းလက်စွဲစာအုပ်ထဲရှိ Social Media ကဏ္ဍတွင်ကြည့်ပါ)

သင်သည် တစ်ခါတစ်ရံ အင်တာနက်ကို တစ်ကိုယ်ရည်အတွက် သုံးစွဲလိုသည်ကို နားလည်ပါသည်။ ရုံးတွင်၊ အလုပ်တွင် ရှိချိန်တွင် FFI ၏ ကွန်ပျူတာများ၊ ပစ္စည်းကိရိယာများ သို့မဟုတ် သင့်ကိုယ်ပိုင် ပစ္စည်းများတွင် အသုံးပြုနိုင်သော်လည်း

- ထမင်းစားချိန် သို့မဟုတ် အလုပ်ချိန်ပြင်ပ တွင်သာ အသုံးပြုပါ။
- လုပ်ငန်းတာဝန်၊ စွမ်းဆောင်ရည်ကို မထိခိုက်အောင် အသုံးပြုပါ။

လုံခြုံမှု

ကျွန်ုပ်တို့၏ ICT စနစ်အပေါ်တွင် သိုလှောင်ထားသော သတင်းအချက်အလက်များနှင့် လုပ်ငန်းစဉ်များသည် နေ့စဉ်လုပ်ငန်းဆောင်တာများအတွက် အလွန့်အလွန်အရေးကြီးပါသည်။ ထို့ကြောင့် အချက်အလက်များနှင့် စနစ်များကို အန္တရာယ်များမှ လုံလောက်စွာ ကာကွယ်ထားရန် မရှိမဖြစ်လိုအပ်သည်။ ထိုအန္တရာယ်များတွင် ပစ္စည်းများခိုးယူခံရခြင်း၊ စနစ်များကို အခွင့်မရှိဘဲဝင်ရောက်ခြင်း၊ အစီအစဉ်များနှင့် အချက်အလက်များကို အခွင့်မရှိဘဲ ကူးယူခြင်း၊ ခွင့်ပြုချက်မရှိသော software အသုံးပြုခြင်းနှင့် သဘာဝ ဘေးအန္တရာယ်များ (ဥပမာ-မီးဘေး၊ ရေဘေးနှင့် လျှပ်စစ်ပြတ်တောက်ခြင်း) စသည်တို့ပါဝင်သည်။ ပစ္စည်း ကိရိယာများနှင့် အချက်အလက်များကို အခွင့်မရှိဘဲ ဝင်ရောက်အသုံးပြုမှုများမှ တတ်နိုင်သမျှ နည်းလမ်း များကိုအသုံးပြု၍ ကာကွယ်ရပါမည်။

ပစ္စည်းကိရိယာလုံခြုံမှု

သယ်ဆောင်သွားနိုင်သော ပစ္စည်းကိရိယာများ (ဥပမာ- laptop, tablet, လက်ကိုင်ဖုန်း) များကို အသုံးမပြုသည့်အချိန်တွင် လုံခြုံသောနေရာတွင် သိမ်းဆည်းထားပါ။ (ဥပမာ- သော့ခတ်ထားသော အံဆွဲ) ရုံးတွင်ဖြစ်စေ၊ အိမ်တွင်ဖြစ်စေ၊ အခြားနေရာများတွင်ဖြစ်စေ ဤကဲ့သို့ကျင့်သုံးပါ။ ကားထဲတွင် ချန်ထားခဲ့ရမည်ဆိုပါက အပြင်ဘက်မှမမြင်နိုင်သည့် ကားအတွင်းဘက်တွင် ထည့်ထားပါ။ အကယ်၍ သေချာစွာ သိမ်း ဆည်းခြင်းမရှိဘဲ ခိုးယူခံရပါက FFI အာမခံမှ ပြန်လည် ပေးအပ်မည်မဟုတ်ပါ။

အချက်အလက်နှင့်စနစ်လုံခြုံမှု

အချက်အလက်နှင့် စနစ်လုံခြုံမှုသည် ကြီးမားသောအန္တရာယ်ရှိနိုင်ပြီး၊ လုံခြုံရေးကျိုးပေါက်မှုမရှိစေရန် FFI သည် အဆင့်များစွာဖြင့် ကာကွယ်ထားသည်။ အချက်အလက်နှင့် စနစ်လုံခြုံမှုအတွက် သင်သည်

- FFI အချက်အလက်များကို တရားမဝင် ဝင်ရောက်ကြည့်ရှုခြင်းကိုကာကွယ်ရန်၊ ကွန်ပျူတာမျက် နှာပြင်ပေါ်တွင် အချက်အလက်များမကျန်ရှိစေရပါ။ (ဥပမာ- log in အသေးစိတ် အချက်အလက် များ၊ passwordများ၊ PIN များ)
- ကွန်ပျူတာ၊ laptop ကွန်ပျူတာနှင့် အခြားပစ္စည်းများကို အသုံးမပြုချိန်တွင် screen ကို lock လုပ်ထားခြင်း၊ log out ထွက်ထားခြင်းများ လုပ်ဆောင်ပါ။
- တစ်နေ့တာလုပ်ငန်းများပြီးဆုံးလျှင် ကွန်ပျူတာမှ application အားလုံးကိုပိတ်ပြီး၊ (sleep သို့မဟုတ် hibernate မလုပ်ဘဲ) လုံးဝ shut down ချကာ၊ power ကို ပိတ်ရမည်။ ထိုသို့ပြုလုပ် ခြင်းဖြင့် မရှိမဖြစ်လိုအပ်သော စနစ်ကာကွယ်ရေး update များအား install လုပ်စေပြီး၊ စွမ်းအင် သုံးစွဲမှုကို လျော့နည်းစေကာ လျှပ်စစ် ကြောင့်ဖြစ်သော မီးဘေးအန္တရာယ်ကို လျော့နည်းစေ သည်။
- အချက်အလက်များအားလုံးကို MyFFI (SharePoint) သင်၏ သက်ဆိုင်ရာ OneDrive Folder သို့မဟုတ် FFI မှ ရွေးချယ်ထားသော အခြားစနစ်များတွင် မူဝါဒအတိုင်းစနစ်တကျ

သိမ်းဆည်းရမည်။ သို့မှသာ ထိန်းသိမ်းထား ပြီးသားဖြစ်သွားပြီး သင့်လျော်စွာ စီမံခန့်ခွဲနိုင်ကာ၊ လိုအပ်ချိန် တွင် အဆင်ပြေစွာ ရယူသုံးစွဲနိုင်မည်။ အချက် အလက်များကို ပုံမှတ်သိမ်းဆည်း ရန်မဟုတ်သော နေရာများ ဥပမာ-ကွန်ပျူတာ၏ desktopများ၊ C: drive များ၊ external hard drives များ စသည် တို့တွင် မသိမ်းဆည်း သင့်ပါ။ အသေးစိတ်ကို Data Management and Retention Policy တွင် ကြည့်နိုင်သည်။

- Malware များ၊ virus များကို ကာကွယ်ရန်၊ မူဝါဒတွင် ဖော်ပြထားသည့်အတိုင်း၊ တရားဝင် software များကိုသာ download ဆွဲပြီး၊ ၎င်းအန္တရာယ်များမှ ရှောင်ရှားနိုင်ရန်အတွက် မူဝါဒ တွင် ဖော်ပြထားသည့်အတိုင်း တရားဝင် သော လုပ်ငန်းကိစ္စများအတွက် အသုံးပြုရပါမည်။
- ကွန်ပျူတာ virus, Trojan, spyware သို့မဟုတ် အခြား malware များကို၊ သိလျက်နှင့် ယူဆောင် သုံးစွဲခြင်း မပြုလုပ်ရပါ။
- ခွင့်ပြုထားခြင်းမရှိသော website များနှင့်စနစ်များကို ဝင်ရောက်သုံးစွဲခြင်း မပြုလုပ်ရပါ။
- လုပ်ငန်းကိစ္စ အတွက် အသုံးပြုသော FFI၏ ပစ္စည်းကိရိယာများနှင့် တစ်ကိုယ်ရည်သုံး ပစ္စည်း များ အားလုံးကို password များ၊ PIN များဖြင့် ကာကွယ်ထားရမည်။
- လုပ်ငန်းကိစ္စအတွက် အသုံးပြုသော FFI၏ စားပွဲတွင် ပစ္စည်းကိရိယာများနှင့် တစ်ကိုယ်ရည် သုံးပစ္စည်းများ အားလုံးကို ခိုးယူချိုးဖောက်မှုများမဖြစ်စေရန် ပစ်ထားခဲ့ခြင်း မပြုလုပ်ရပါ။

Email လုံခြုံစွာအသုံးပြုခြင်းလမ်းညွှန်ချက်ကို Creation, Use and Retention of FFI Email Accounts Policy and Procedure တွင် ကြည့်နိုင်သည်။

အများပြည်သူနှင့်သက်ဆိုင်သောနေရာများ

သင့်ပစ္စည်းကိရိယာနှင့် FFI network ကို ဝင်ရောက်အသုံးပြုခြင်း သို့မဟုတ် အများပြည်သူသုံး Wi-Fi connection (ဥပမာ-ကော်ဖီဆိုင်၊ လေဆိပ် သို့မဟုတ် ဟိုတယ် Wi-Fi) ကိုအသုံးပြုလျှင်၊ လိုက်နာရန် များ မှာ

- Windows firewall ကို ဖွင့်ထားပါ။ (နောက်ဆက်တွဲ ၁ ကိုကြည့်ပါ)
- File sharing ကို ပိတ်ထားပါ။ (နောက်ဆက်တွဲ ၂ ကိုကြည့်ပါ)
- အများပြည်သူသုံး Wi-Fi ဖြင့် software update များကို၊ (လုပ်ခိုင်းသော်လည်း) မပြုလုပ်ပါ နှင့်။
- အသုံးမပြုတော့လျှင် Wi-Fi connection ကိုပိတ်ထားပါ။
- Hotspot များအသုံးပြုလျှင် Free Wi-Fi သို့မဟုတ် Free Hotel Wi-Fi များကို သတိကြီးစွာ ထားပါ။ ၎င်းတို့သည် ဟက်ကာများမှ သင့် device ထဲသို့ ဖောက်ဝင်နိုင်ရန် ထောင်ထားသော network အတုများဖြစ်နိုင်သည်။ အချိန် အနည်းငယ်ပေး၍ ဟိုတယ် သို့မဟုတ် လေဆိပ် WiFi စသည်တို့ ကိုသာ ရှာဖွေပြီး network log on ဝင်ရောက် ကာ အသုံးပြုပါ။
- လုံခြုံရေးအားနည်းသော ကြိုးမဲ့ဧရိယာများတွင် လျှို့ဝှက်သင့်သောအကောင့်များ ဝင်ရောက်မှု မှ ရှောင်ကြဉ်သင့်သည်။ (ဥပမာ - ဘဏ်အကောင့်များ)
- အများပြည်သူသုံး network ဖြင့် ဘဏ်လုပ်ငန်းဆိုင်ရာနှင့် အခြားလျှို့ဝှက်သတင်း အချက် အလက်များ ကို သုံးစွဲမှုရှောင်ကြဉ်ပါ။

သတိပြုရန် - Web page အမည်၏ အရှေ့တွင် https ၏ အဓိပ္ပာယ်သည် ထို website သည် 'သက်ဆိုင်သူများသာ ဖတ်ရှုနားလည်မည့် ကုဒ်ပြောင်းထား'(encrypted) ပြီး၊ ကြားလူဝင်ရောက်ဖတ်ရှု၍ မရနိုင်ပါ။ Web page အမည်၏ အရှေ့တွင် http ၏ အဓိပ္ပာယ်သည် ထို website သည် 'သက်ဆိုင်သူများသာ ဖတ်ရှု နားလည်မည့် ကုဒ်ပြောင်းမထား' (not encrypted) ကာ၊ ကြားလူဝင်ရောက်ဖတ်ရှု၍ ရနိုင်သည်။ ထို့ကြောင့် သင်သည်လျှို့ဝှက် ထိန်းသိမ်းအပ်သော သတင်းအချက်အလက် (ဥပမာ- ကဒ်နှင့်ငွေပေးချေ ခြင်း) ကိုပို့ရန် http site ကို အသုံးပြုလျှင် ထိုသတင်းအချက်အ လက်သည် ကြားမှ မြင်တွေ့နိုင်သည်။ မကြာခဏဆိုသလို http site ကို စတင်ဝင်ရောက်ပြီး၊ ပေးချေမှုကိုပြုလုပ် လိုက်လျှင်၊ https site သို့ပြောင်းလဲရောက်ရှိသွားသည်။ သတိပြုပါ https site တွင် web address ၏ဘေးတွင် သော့ခလောက် ပုံလေးပါရှိသည်။ လိုအပ်၍သိရှိလိုပါလျှင် website certificate ကို စစ်ဆေးကြည့်နိုင်သည်။ သော့ခလောက်ပုံလေးကို နှိပ်ကြည့်လျှင် လုံခြုံရေးအချက်အလက်များကို တွေ့နိုင်ပြီး၊ certificate သက်တမ်း ရှိနေ သေးကြောင်း၊ certificate လမ်းကြောင်း နှင့် အခြေအနေကို သိရှိနိုင်သည်။ (နောက်ဆက်တွဲ ၃ ကိုကြည့်ပါ)

Password မူဝါဒ

လုပ်ငန်းကိစ္စများအတွက် အသုံးပြုသော FFI မှ ပစ္စည်းများနှင့် တစ်ကိုယ်ရည်သုံးပစ္စည်းများတွင် password နှင့် ကာ ကွယ်ထားရမည်။ (သို့မဟုတ် PIN အသုံးပြုရမည်) ရွေ့လျားစက်ပစ္စည်းများ၊ ကွန်ပျူတာများ၊ တစ်ကိုယ်ရည်သုံး ကွန်ပျူတာများ၊ တက်ဘလက်များနှင့် လက်ကိုင်ဖုန်းများ အားလုံးတွင် အသုံးပြုရမည်။

အချက်အလက်များနှင့် စနစ်များကို ကာကွယ်ရန်

- ရက်ပေါင်း (၉၀)လျှင် တစ်ကြိမ် password ချိန်းရမည်။ (နောက်ဆက်တွဲ ၄ ကိုကြည့်ပါ)
- ပထမအကြိမ်အသုံးပြုထားသည့် password ကို ပြန်မသုံးရ
- သင့်အမည်မှစကားလုံးများ သို့မဟုတ် သင့်emailလိပ်စာ သို့မဟုတ် emailလိပ်စာမှ စကားလုံးများကို နှစ်ကြိမ်ဆက်တိုက် ပြန်လည်အသုံးမပြုရ။
- အမည်များကို မထည့်သွင်းရ
- ကိုယ်ရေးကိုယ်တာကိစ္စရပ်များအတွက် အသုံးပြုနေသော password များ ထပ်မံအသုံးမပြုရ။
- အားကောင်းသော password ကို ဖန်တီးရန်၊ အောက်ပါတို့မှ အနည်းဆုံးလိုအပ်ချက်များ အားသုံးပြီး password (လျှို့ဝှက်စာလုံး) အား အနည်းဆုံး (၁၀)လုံး ဖန်တီးပါ။
    - အင်္ဂလိပ်စာလုံးအကြီးများ (A through Z)
    - အင်္ဂလိပ်စာလုံးအသေးများ(a through z)
    - အခြေခံ ဂဏန်းလုံး ၁၀ လုံး(0 through 9)
    - အက္ခရာမဟုတ်သော သင်္ကေတများ (for example, !, $,#, %)
- အခြားသူများ (Third Party) သို့ အသုံးပြုသော အမည်၊ password များ မပြောရ။

စနစ်အရ ၅ ခါများဝင်ပြီးလျှင် email account ဖွင့်၍မရတော့ဘဲ lock ကျသွားပါမည်။ ictsupport@fauna-flora.org ကို email ပို့ပြီး ICT အကူအညီကို ရယူပါ။
Password ကို reset ချရန်အတွက် ICT အကူအညီယူရန် email ပို့သည့်အခါ သက်ဆိုင်ရာ မန်နေဂျာ ကိုမိတ္တူထည့်ပို့ပါ။ မန်နေဂျာမှ မှန်ကန်ကြောင်း ထောက်ခံပေးရန်လိုပါသည်။ သင်သည် password ကို reset ချခိုင်း သည်ကို သံသယ ရှိပါက ICT support ကို တိုက်ရိုက်ဆက်သွယ်ပါ။
ICT support ထံမှ ယာယီ password အသစ် လက်ခံရရှိပါက မူဝါဒအရ ၂၄ နာရီကျော်မှ reset ပြန် လုပ်သင့်သည်။

အဝေးရောက်အလုပ်လုပ်ခြင်းနှင့် Password များ

အကယ်၍ သင်သည် UK တွင် အခြေစိုက်ပါက သင်၏ laptop သို့မဟုတ် ကွန်ပြူတာသည် FFI Domain နှင့် ချိတ်ဆက် ထားသည်။ အကယ်၍သင်ခရီးထွက်နေချိန်တွင် password expire ဖြစ်သွားပါက၊ Outlook နှင့် MyFFI ကို ဝင်ရောက် ရန် password အဟောင်း ကို အသုံးပြုကာ Log in ဝင်ပြီး password အသစ်ကို ပြုလုပ်ကာ ဝင်ရောက်ရမည်။ UK ရုံးသို့ ပြန်ရောက်သောအခါ သင်၏ laptop သည် FFI domain နှင့် sync ဖြစ်သွားပြီး၊ password အသစ်ကို အသုံးပြုကာ log in ဝင်ရောက်ရမည် ဖြစ်သည်။
အခြားနိုင်ငံရုပ်ခြားတွင် အလုပ်လုပ်ပါက သင်၏ laptop၊ ကွန်ပြူတာသည် FFI domain နှင့် မချိတ်ထားပါ။ သင့်ထံတွင် password နှစ်ခုရှိမည်ဖြစ်ပြီး၊ တစ်ခုသည် laptop အား login ဝင်ရန်နှင့် နောက်တစ်ခုမှာ Outlook နှင့် MyFFI (SharePoint) ကို ဝင်ရောက်ရန်ဖြစ်သည်။
သင်၏ အချက်အလက်များကို လုံခြုံနေစေရန် အားကောင်းသော password ကို အမြဲတမ်း ဖန်တီးရန် နှင့် ပုံမှန်ပြောင်းလဲပေးရန် လိုအပ်သည်။

ဖိုင်များကို ပြင်ပအဖွဲ့အစည်းများသို့ မျှဝေသုံးစွဲခြင်း

ဖိုင်များအားပြင်ပသို့ မျှဝေသုံးစွဲရာတွင် သင်သည်

- သင်၏ FFI OneDrive ထဲသို့ ဦးစွာ သိမ်းဆည်းပြီးနောက်FFIပြင်ပမှ ပုဂ္ဂိုလ်ထံ email ဖြင့် ပေးပို့ မျှဝေရမည်။ OneDrive အသုံးပြုနည်းကို (Sharing Documents) ဖိုင်များမျှဝေခြင်း လမ်းညွှန် ချက်ကို ကြည့်ပါ သို့မဟုတ် အသိပညာစီမံခန့်ခွဲမှု အရာရှိ၏ အကူအညီကို ရယူပါ။
- သတ်မှတ်ထားသော ဝန်ဆောင်မှုဖြင့်သာ ဖိုင်များကို upload လုပ်ပြီး မျှဝေပါ၊ အထက်တွင် အကျယ်တဝင့် ဖော်ပြထားသော လုံခြုံရေး ကိစ္စများကြောင့် Dropbox မှ တဆင့် မမျှဝေပါနှင့်။

Email

FFI ၏ Creation, Use and Retention of FFI Email Accounts Policy and Procedure ကို ကြည့်ပါ။

Skype

အလုပ်တွင်လုပ်ငန်းကိစများကို Skype, Skype for Business နှင့် အခြား messaging facility များ အသုံးပြု၍လည်း ဆက်သွယ်ဆောင်ရွက်နိုင်သည်။ email ကဲ့သို့ပင် ထို instant message များသည် ဆက်သွယ်ထားသည်များအား စာရွက်စာတမ်းများကဲ့သို့ ပုံသေမှတ်တမ်းများ ကျန်ရှိခဲ့ပြီး မှီငြမ်းနိုင်သည်။ ထိုသို့ဆက်သွယ်ရာတွင် သင့်လျော်သော၊ ပညာရှင်ဆန်သော၊ လေးစားမှုရှိသော၊ လျှို့ဝှက်မှုကို ထိန်းသိမ်း သော ဆက်သွယ်မှုများ ဖြစ်ရန် အရေးကြီးသည်။

ဖုန်း၊ တက်ဘလက် များ

FFI UK ရုံးတွင်အခြေစိုက်ပါက၊ ပုံမှန်အားဖြင့် FFI လိုင်းဖုန်းများ တပ်ဆင်ပေးထားသည်။ FFI လက်ကိုင်ဖုန်းကို ပံ့ပိုးထားသူများလည်းရှိသည်။ FFI လက်ကိုင်ဖုန်းကို အသုံးပြုရပါက၊ လမ်းညွှန် အသေးစိတ်ကို FFI ၏ Mobile Phone Policy ကို ကြည့်ပါ။ ဝန်ထမ်းများအားလုံးအတွက် electronic phone manager software ကိုလည်း အသုံးပြုရမည်။

FFI ဖုန်းများကို FFI လုပ်ငန်းများဆောင်ရွက်ရန် ပံ့ပိုးပေးထားခြင်းဖြစ်သည်။ သို့သော် သင်သည် တစ်ခါတစ်ရံ ကိုယ်ရေးကိုယ်တာကိစ္စ ဖုန်းပြောဖို့လိုအပ်မည်ကို နားလည်ပါသည်။ ထိုအချိန်မျိုးတွင်

- ဖြစ်နိုင်လျှင် တစ်ကိုယ်ရည်သုံးဖုန်းကို အသုံးပြုပါ
- ဖြစ်နိုင်လျှင် ကိုယ်ရေးကိုယ်တာဖုန်းပြောမှုကို ထမင်းစားချိန်တွင်သာ ပြုလုပ်ပါ
- သင်၏ လုပ်ငန်းများနှင့် စွမ်းဆောင်ရည်ကို အနှောင့်အယှက် မဖြစ်ပါစေနှင့်
- သင့်ကြောင့် လုပ်ငန်းဝန်းကျင်ကို အနှောင့်အယှက် မဖြစ်ပါစေနှင့်

သင်ရုံးပြင်ပရောက်နေချိန်များတွင်၊ ဖုန်းဖြေကြားမှု မပြုလုပ်နိုင်သည့် အချိန်များတွင်၊ ရုံးပြင်ပရောက်နေကြောင်း အလိုလျောက်ဖြေကြားမှုကို အသုံးပြုသင့်သည်။ ရုံးတွင်သင်မရှိသည့် ရက်စွဲ၊ အချိန် နှင့် မည်သည့်အချိန်တွင် အဆင်ပြေကြောင်းနှင့် ထိုအချိန်အတွင်း မည်သူနှင့်ဆက်သွယ်နိုင်ကြောင်းကို အသိပေးနိုင်သည်။ သင်၏ voice mail ကို ပုံမှန်စစ်ဆေးသင့်ပြီး၊ message များကို သင့်လျော်သလို ပြန်ကြားရမည်။

အကယ်၍သင်သည် လုပ်ငန်းကိစ္စများအတွက် တစ်ကိုယ်ရည်သုံးဖုန်း သို့မဟုတ် တက်ဘလက် ကို အသုံး ပြုပြီး FFI email account နှင့် SharePoint ကို ဝင်ရောက်အသုံးပြုလိုပါက၊ ဤမူဝါဒအရ သင့်ပစ္စည်းနှင့် ပါဝင်သောအရာများ၏ လုံခြုံရေး ကို သေချာစေရန် PIN ဖြင့် ကာကွယ်ထားရမည်။

ဆက်သွယ်မှုများကို စောင့်ကြည့်လေ့လာခြင်း

FFI သည် အချိန်မရွေး သင်၏ အလုပ်ကိစ္စအတွက် အင်တာနက်အသုံးပြုမှု၊ လူမှုကွန်ယက်၊ email နှင့်၊ သို့မဟုတ် ဖုန်းပြောဆိုမှု များကို အချိန်မရွေး စောင့်ကြည့်လေ့လာနိုင်သည်။ အဘယ်ကြောင့်ဆိုသော်

- ဖန်တီးလိုက်သော အချက်များသည် FFI နှင့် ကိုက်ညီမှုရှိစေရန်
- FFI ၏ မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများကို လိုက်နာရန်
- သင့်လျော်သော စံသတ်မှတ်ချက်များ နှင့်ကိုက်ညီစေရန်
- ခွင့်ပြုချက်မရှိသော သုံးစွဲမှုများ၊ တလွဲသုံးစွဲမှုများကို စုံစမ်းသိရှိနိုင်ရန်
- ICT စနစ်များ ထိရောက်စွာ ဆောင်ရွက်နိုင်စေရန် (ဥပမာ- virus စောင့်ကြည့်ခြင်း)

- ရာဇဝတ်မှုများကို ကာကွယ်နိုင်ရန်နှင့် စုံစမ်းနိုင်စေရန် တို့အတွက်ဖြစ်သည်။

တစ်ကိုယ်ရည်သုံး email များကို မှတ်သားထားရန်နှင့် တစ်ကိုယ်ရည်သုံး email ကို ပို့လာသူများကိုလည်း ထိုသို့သတ်မှတ်ပြီးပို့ရန် ပြောထားသင့်သည်။ FFI သည် စောင့်ကြည့်လေ့လာရာတွင် တစ်ကိုယ်ရည်သုံး email များကိုရှောင်သွား နိုင်မည်ဖြစ်သည်။ မည်သို့ပင်ဖြစ်စေ FFI email account ကို အသုံးပြုပြီး တစ်ကိုယ်ရေ email များကို အသုံးပြုရန် အခွင့်မရှိပါ၊ သုံးခဲ့လျှင်လည်း privacy လုံခြုံမှုအတွက်မျှော်လင့် ၍ မရနိုင်ပါ။

ပြန်လည်သုံးသပ်ခြင်း

ဤမူဝါဒကို အချိန်မရွေးပြန်လည်သုံးသပ်ပြီး ပြင်ဆင်နိုင်ခွင့်ရှိသည်။

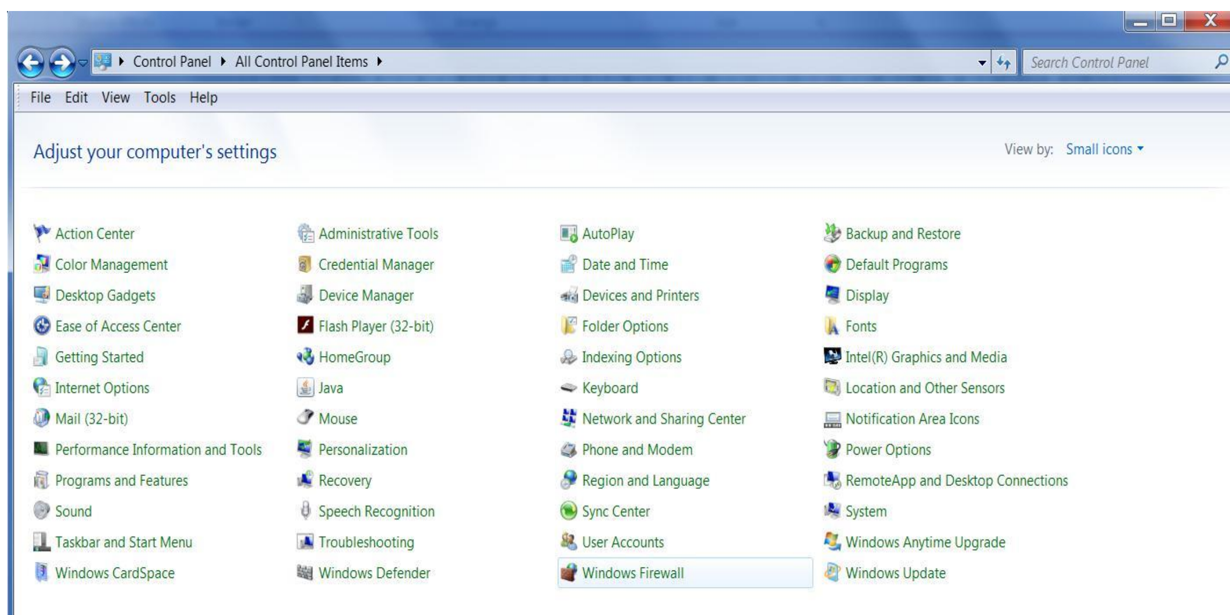
နောက်ဆက်တွဲ (၁)

Firewall ကို ဖွင့်ခြင်း

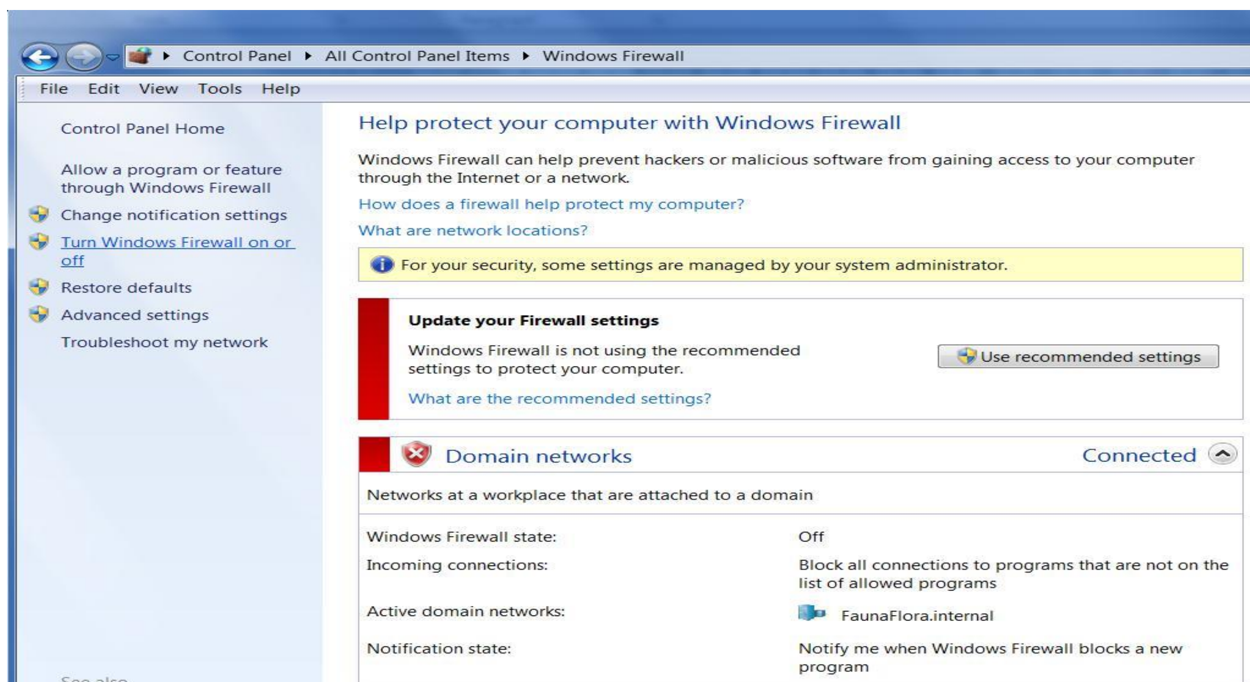
Start မှ - Control Panel မှ - Change view မှ view by: Small Icons



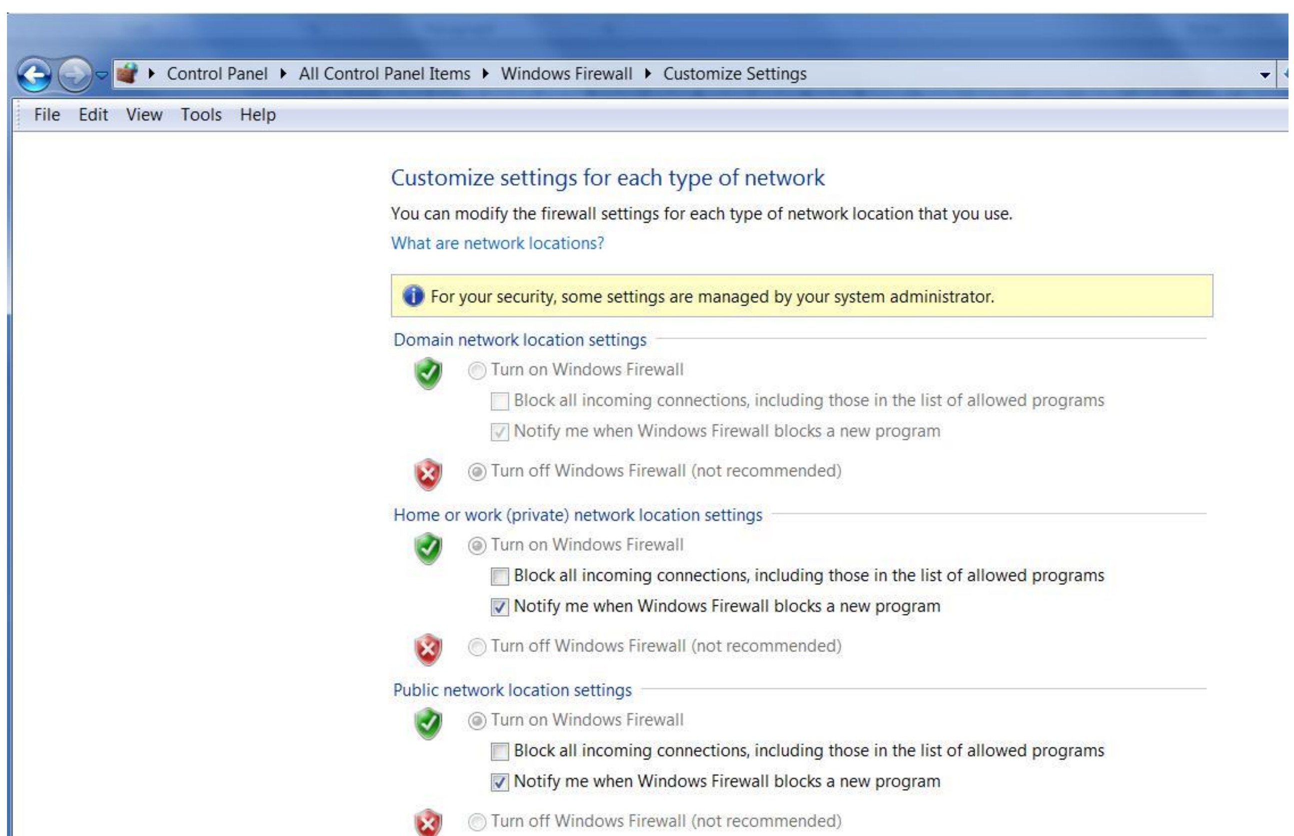
Windows Firewall ကိုနှိပ်ပါ



Turn Windows Firewall on or off ကိုရွေးပါ (ဘယ်ဘက်အခြမ်းတွင်ရှိသည်)



turn on ကို နှိပ်ပါ



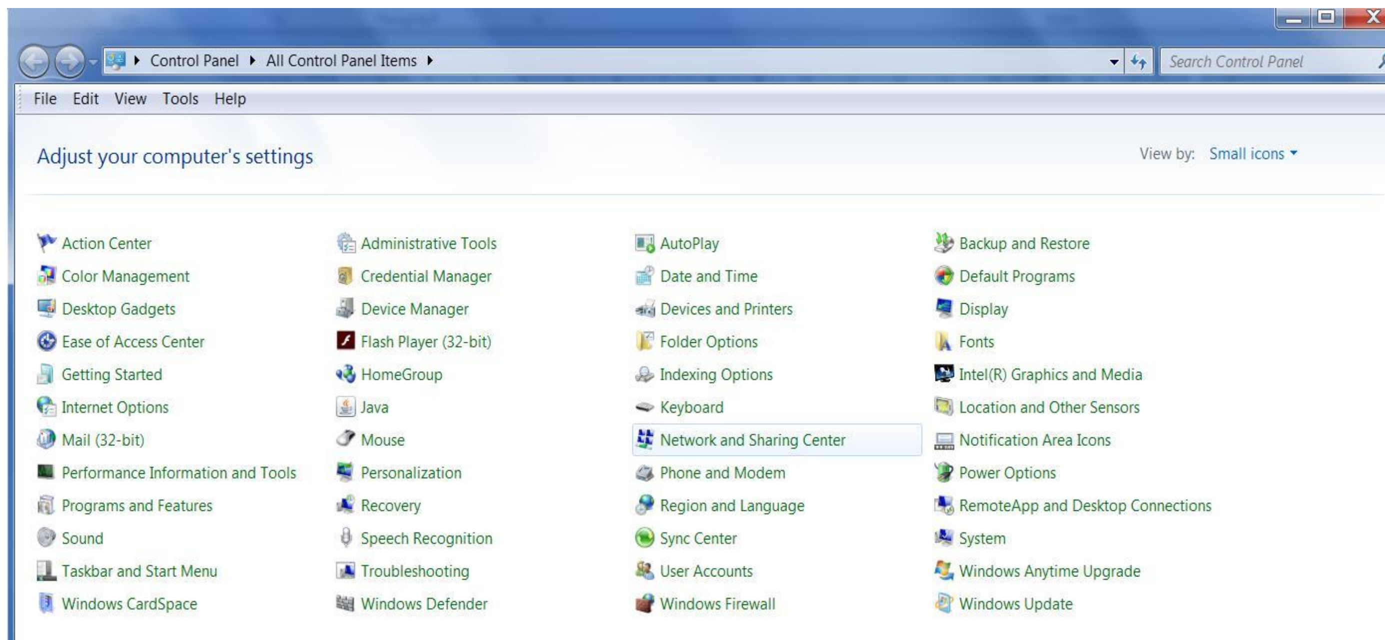
နောက်ဆက်တွဲ (၂)

File Sharing ကို Turn off လုပ်ခြင်း

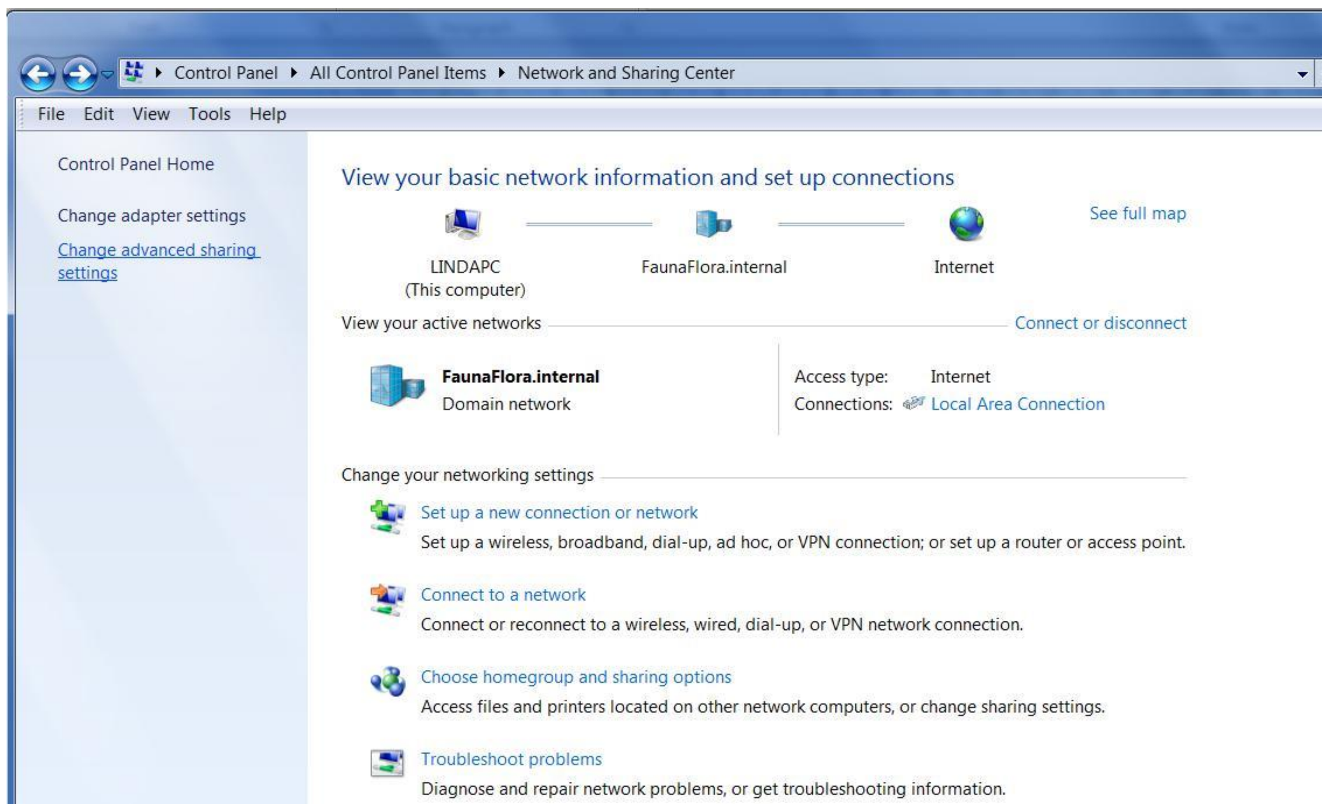
Start မှ – Control Panel မှ – change view မှ view by: Small Icons



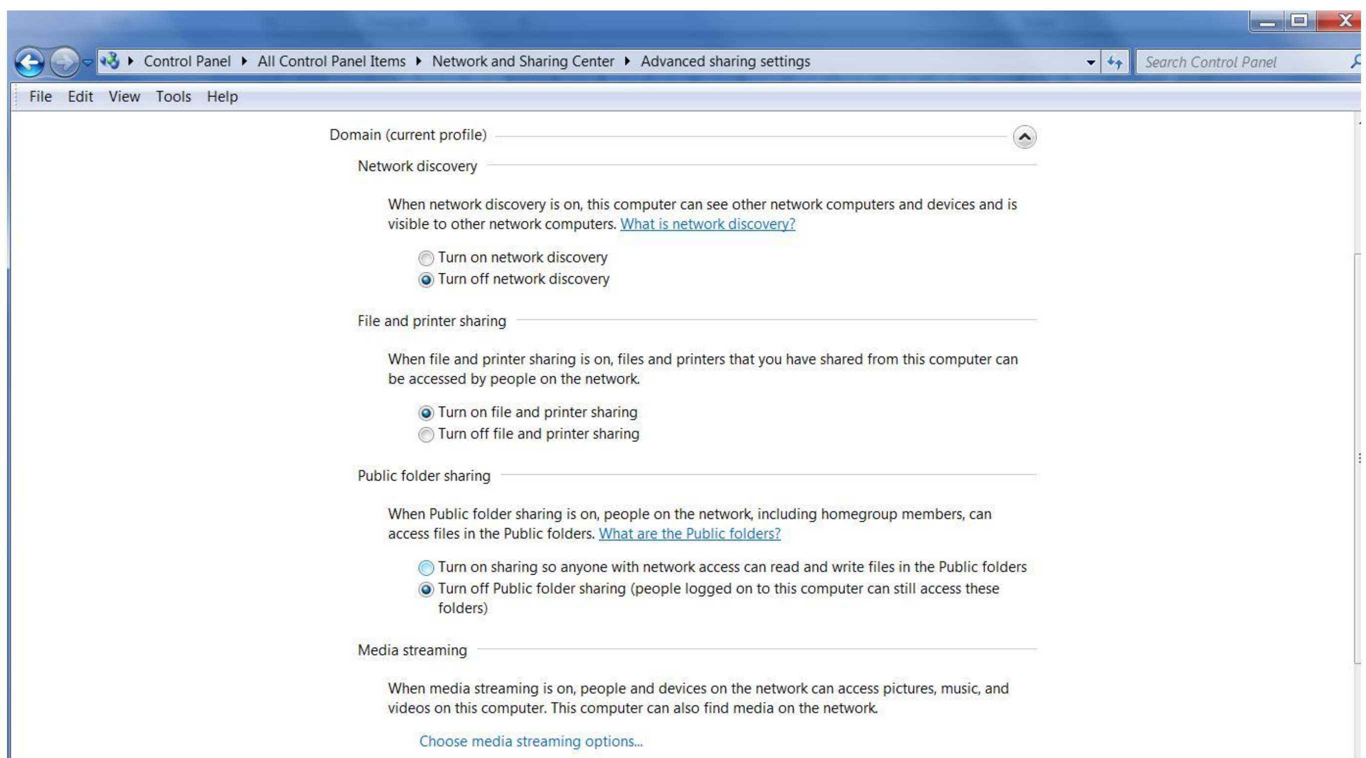
Network and Sharing Center ကို ဖွင့်ပါ



Change Advanced Sharing Settings ကို နှိပ်ပါ (ဘယ်ဘက်အခြမ်း)

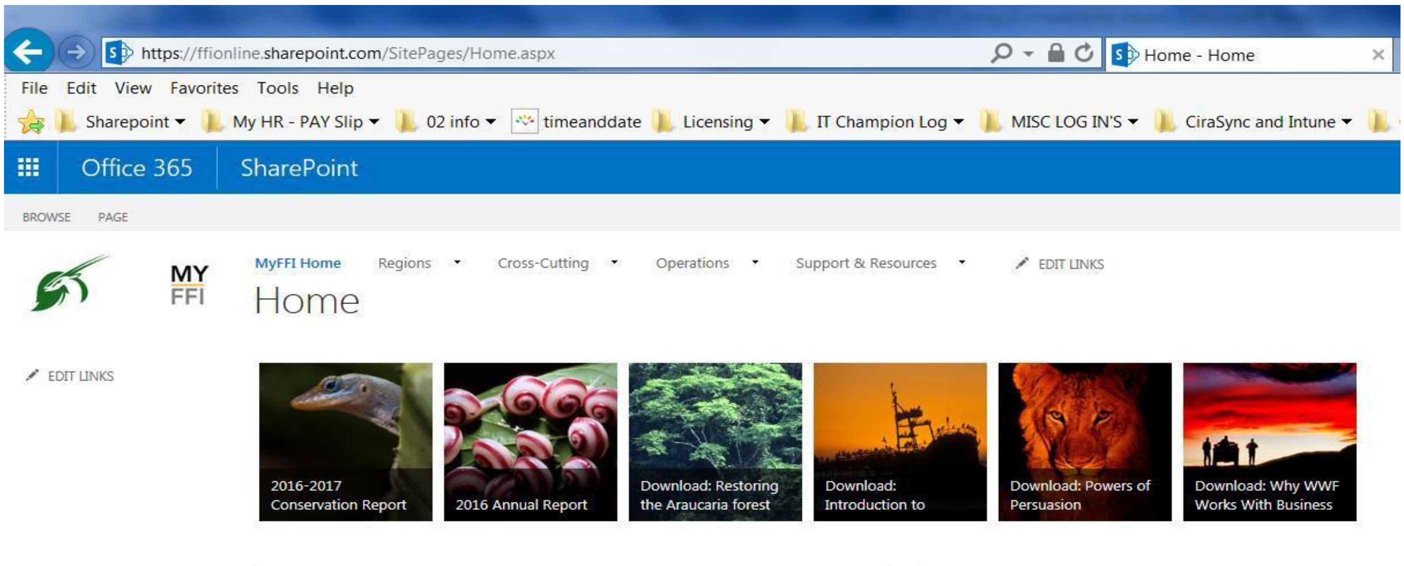


Public Heading အောက်တွင် File sharing ကို turn off လုပ်ပါ

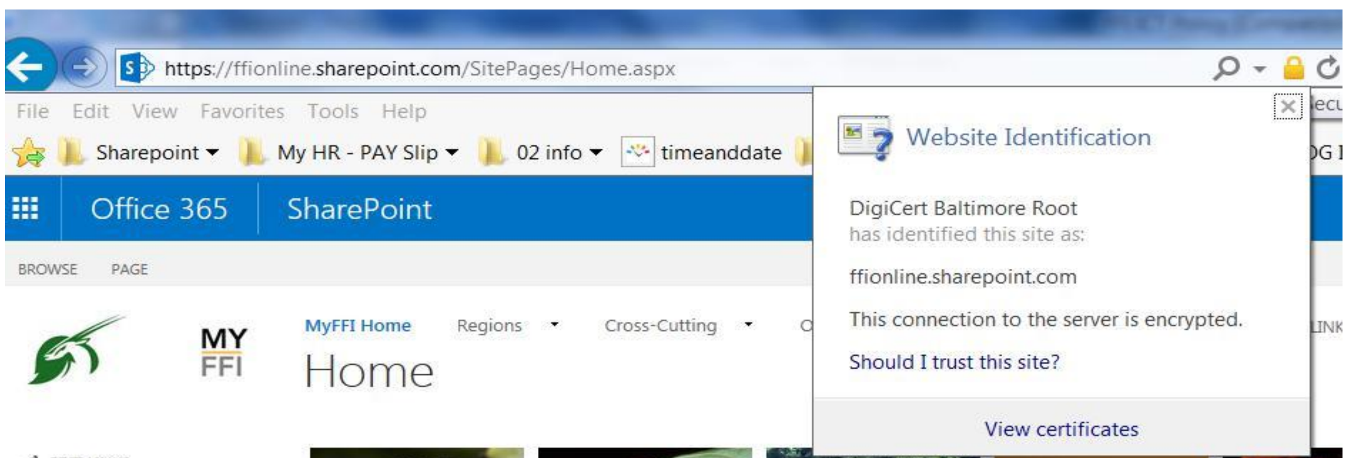


နောက်ဆက်တွဲ (၃)

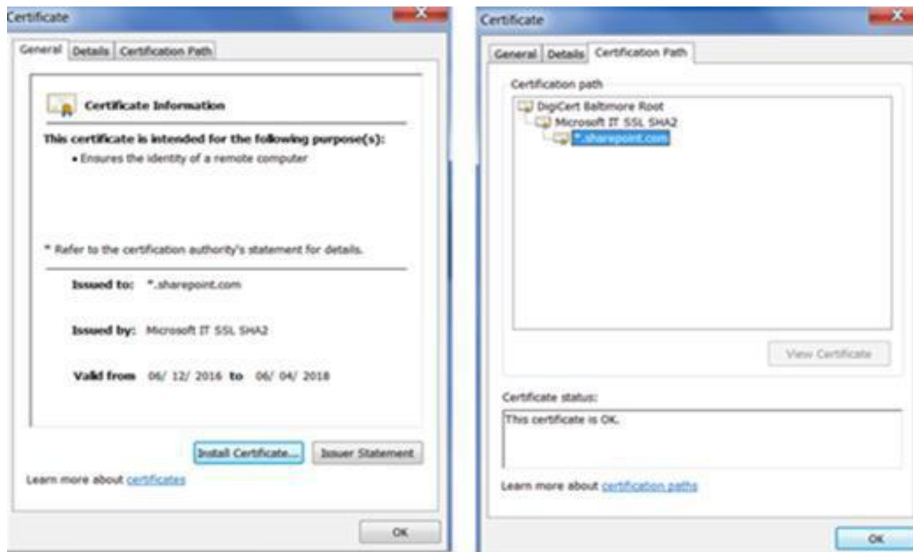
လုံခြုံသော website များ
https://



URL (website name) ၏ အဆုံးတွင် သော့ခလောက်ပုံလေးကို နှိပ်ပါ



View certificates ကိုနှိပ်လျှင် certificate အချက်အလက်များနှင့် လမ်းကြောင်းနှင့် တရားဝင်ကြောင်း တွေ့ရမည်။



(ဘာသာပြန်လိုအပ်ချက်ကြောင့် အဓိပ္ပာယ်တစုံတရာ ကွဲလွဲမှုရှိခဲ့သော် အင်္ဂလိပ်စာဖြင့်ရေးသားထားသော မူရင်းသည်သာ အတည်ဖြစ်သည်။)

ကျွန်ုပ်သည် အထက်ပါ "**သတင်းအချက်အလက်နှင့် ဆက်သွယ်ရေးနည်းပညာ (ICT) မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်း**" အား ဖတ်ရှုနားလည်ပြီး လိုက်နာပါမည်ဟု ကတိကဝတ်ပြုလျက် အောက်တွင် လက်မှတ်ရေး ထိုးပါအပ်သည်။

လက်မှတ် -

အမည် -

ရက်စွဲ -